2600

BBS BUST, TRACKING DEVICES, 800 DIRECTORY, REMOTE METER READING, INTRO TO HACKING, ISRAELI PHONES, WIRETAPPING NEWS, IRS VS. TELCO, AND MUCH MORE!

JUNE, 1985

VOLUME TWO, NUMBER SIX

2600 is published by 2600 Enterprises, Inc., an eleemosynary organization.
Subscription rates: [illegible] Lifetime subscription: [illegible] Corporate sponsorship: [illegible] Make checks payable to: 2600 Enterprises.
Write to: 2600, Box 752, Middle Island, NY 11953-0752. [illegible] ISSN [illegible]

a guide to the israeli phone system

The Israeli phone system, like their AC current (220 volts) and their television standard (PAL) is a European system. European telephones differ from the American standard in several interesting ways. First of all, dialing is by shorting out the phone line rather than opening it up. One of the drawbacks of this method is that an extension phone on a line being dialed will have its bell capacitors continually discharged and recharged during the dialing, making a little "ping" for each dialing pulse. Good if you want to know about activity on the line, bad if you don't want someone else's dialing to bother you. Another difference is the "off hook" voltage -- a mere 3.5 volts, compared to the heftier 7-9 volts in an American system.

Their pay telephones are organized on a token system. You throw in one token for a local call, and for longer distances the pay phone eats the tokens at a certain rate per minute. There's a little chute in the phone which will stack up four or five of the tokens so that you don't have to pour them in all the time. ASEMONIM (which is just the Hebrew word for "tokens") can be bought at any post office. The going rate is around a nickel each.

This system has various advantages and drawbacks. The pay telephone doesn't have to be very complicated. All it does is disable the dial until you've dropped at least one token in, and cut you off when the tokens run out. Whether or not the tokens drop into its coin box (unused tokens can be retrieved when the call is over) is determined by the exchange. Signals are sent over one of the three wires of the pay phone's line whenever the exchange decides that it wants another token. Just disconnecting the proper wire (which can happen by itself at times when the phone breaks down) will let the phone run forever on one token. Worse yet, if you can access the two other wires of the payphone's line, you can clip on your own telephone and dial away with no restrictions. Various other schemes exist that mechanically jam the tokens in one way or another so that they just don't drop down into the coin box and the call is never cut off. Not only that, but if you're good with the hookswitch, you can dial the number yourself without dropping tokens in at all! The payphone dial won't dial until you chuck a token in, but hand-pulsing the hookswitch, though a tedious process, can get you connected. It only makes sense for local calls, though, since on any other kind the payphone will cut you off when the exchange asks for another token. And it makes a lot of noise and looks suspicious, and with the clumsy hookswitches provided, is not very accurate.

With making free calls (or almost free, for one token) so easy, one wonders how their telco takes any money in at all. The explanation lies in their rate structure, which is rather reasonable. There are only three mileage rates: local, which is one message unit (or one telephone token from a pay phone), intermediate (say, from the center of town to the remote suburbs of that town), and long distance (from one city to another). That's it. So to call from one city to another, whether they are separated by fifty kilometers or a few hundred, is still the same rate. So even phone calls between remote corners of the country don't add up that quickly. And on a one token local call, you can talk all you want. So in general, there's not that much of a need to steal calls from pay phones, since the token supply is plentiful and low-priced.

Of course, those perhaps artificially low rates don't apply to international calls. The Israeli solution is rather simple: you can only make collect international calls from a pay phone. Not only that, you have to spend a couple of tokens in the process. You're forced to call a Tel Aviv number where an operator will take your number and (hopefully) call you back. During peak periods, it becomes almost impossible to reach this operator. Even if you get through the busy signal, they don't always answer immediately (and the calling exchange automatically disconnects the call after a minute and a half if no billing signal is received, so you can't ring their phone for any decent length of time. This also takes most of the fun out of calling a black box in another country, since you invariably get cut off within two minutes. Black boxes don't seem to work locally, as the exchange doesn't switch the audio in until someone is paying for the call -- this often results in the first "Hello?" getting cut off). You can usually dial international calls direct from a home phone, but if you need an international operator then the service is almost as bad.

Just getting a home phone in the first place can be a long hassle. When you first get your own phone, you must pay around $350 for an initiation fee. But after that, no matter how many times you move or need the phone reinstalled, there aren't any more connection charges. But if you live in a newly built area where the phone lines haven't been laid yet, you can wait several years (!) to have your service installed. Even if you move into an apartment that already has a line installed the wait can be as long as several months. This situation is supposed to be improving, though, especially with the installation of electronic switching exchanges that have large capacities. In areas with overburdened exchanges, party lines are also very common, and are often the only service available. Party lines there are nowhere near as much

(continued on page 2-38)

Sherwood Forest Shut Down by Secret Service

An All Too Familiar Story

Yes, it's happened yet again. This time, two of the most prestigious computer hacker bulletin boards around, Sherwood Forest II and III, were raided by the government. The by now familiar scene of law enforcement types shutting down a bulletin board system because somebody didn't like what they'd been saying is no longer even newsworthy, judging from the complete lack of media coverage. That is probably the most worrisome ingredient here.

On this occasion, it wasn't the FBI that carried out the raids, but the Secret Service. Why? According to William Corbett in the Washington public affairs office, the Secret Service became authorized to conduct these investigations after October 1984 under United States Codes 1030 (fraud by wire) and 1092 (credit card fraud). Because it's still an "active investigation", Corbett declined to give out any details on the case.

Bioc Agent 003, a co-sysop on Sherwood Forest II, claims that warnings were posted all over the board concerning the posting of credit card numbers. "The management didn't have enough time to constantly look after the system," he said. He attributes the raids to "schmucks that posted numbers anyway". He also believes that posted information on credit firms (CBI and TRW) led to the seizures.

As an example of the kind of muterial Sherwood Forest had availuble, we are reprinting one of their articles below. We feel this one is particularly timely and ironic. In addition, we are running one of their many hacker guides on page 2-40. We will run others in the future. If you'd like to send us a copy of a Sherwood Forest article that we may not have, please do. We must not allow them to be silenced forever.

SOME WORDS ON HACKER MORALITY

A lesson in phreaking and hacking morality:

I find it truly discouraging when people, intelligent people seeking intellectual challenges, must revert to becoming common criminals. The fine arts of hacking and boxing have all but died out. Though you newcomers, you who have appeared on the scene in the last year or two, may not realize it, we had it much better. People didn't recognize our potential for destruction and damage because we never flaunted it, nor did we exercise it.

For hacking, it was the intellectual challenge which drove us to do it. The thrill of bypassing or breaking through someone's computer security was tremendous. It wasn't a case of getting a password from a friend, logging on, and destroying an entire database. We broke in for the challenge of getting in and snooping around WITHOUT detection. We loved the potential for destruction that we gave ourselves, but never used.

Today, after so much publicity, the fun has turned to true criminality. Publicity we have received is abhorring. From WarGames to the headlined October Raids, to the 414's, the Inner Circle, Fargo 4a, and the NASA breakins--not to mention all the local incidents that never made the big newspapers, like break-ins at school computers or newspaper computers. TRW credit information services claims hackers used three stolen accounts to aid them in abusing stolen credit cards. The thrill of entering and looking around has shifted to criminal practicality--how can I make my bank account fatter--how may I use this stolen credit card to its fullest--how could I take revenge upon my enemies.

And then there is the world of Phone Phreaking. The number of phreaks has grown from an elite few, perhaps ten or twenty, to well over a thousand. Still, there remain only about 10 or 20 good, longlasting phreaks. The rest receive information and abuse its uses until the information is no longer valid. Even worse, they seek publicity! They WANT to be caught! Many even use their real names on bulletin board systems to promote publicity. Meanwhile, the REAL phone phreaks have been resting in the shadow of the rest, waiting for phreaking to become so dangerous as to become a challenge once again. Once security tightons and only the strong survive (phreak Darwinism?), phreaking will be restored as a way to 'beat the system' without costing anyone anything.

Hacking may soon be dead, but may phone phreaking live on!

Big Brother [Courtesy of Sherwood Forest][-- (914) 359-1517]

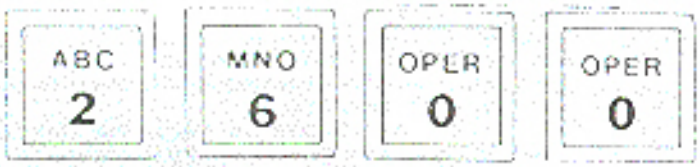
Out of the Inner Circle—A REVIEW

Out of the Inner Circle. A hacker's guide to computer security. By "The Cracker" Bill Landreth, The teenage computer wizard apprehended by the FBI. $9.95, Microsoft Press.

Out of the Inner Circle is one of the many books written by former criminals, but probably the first written by a former hacker or should it be reformed hacker. It is written for middle level managers and for those who want to hear Bill Landreth describe how a hacker thinks. It only describes so called hacker computer crime as opposed to hard core white collar crime, where people scheme to steal secrets or large sums of money. Landreth tries to avoid being too technical for the benefit of his readers, those who are making many of the decisions that affect security, and so he can present his guide to computer security without having to detail all possible procedures for the many different systems that exist today.

In it he describes the beginning of The Inner Circle, which was a group of hackers who were dedicated to peaceful and non-destructive hacking and were subsequently decimated with other groups, like PHALSR, by the Telenet busts of 1983. He surveys the history of hacking and the evolution of the home computer in order to present his profile of a hacker and the motivating forces behind the hacker. This

(continued on page 2-38)



FLASH

Bell Didn't Invent Phone?

The Associated Press

Antonio Meucci is credited by some as the true inventor of the telephone. Meucci, who reportedly could not afford the $10 for a temporary patent back in 1873, was honored by Italian-Americans in Meucci Square. The 177th anniversary of Meucci's birth was heralded by John LaCorte, who said "If he'd had the $250 (for a permanent patent) then, the world would call it Meucci Telephone today, not Bell Telephone."

One of six inventors racing to invent the telephone, Meucci publicly showed sketches of his designs used in the temporary patent in hopes of attracting investors, but to no avail, LaCourte said. LaCourte added that Bell patented the telephone based entirely on Meucci's electrical designs.

The only remaining tributes to Meucci are the square off Avenue U and 86th Street in Brooklyn and the little-known Garibaldi-Meucci Museum on Staten Island. The square, incidentally, is across from the Bell Telephone Co. Building.

The Italian Historical Society of America unsuccessfully sued in 1976 to enjoin the Postal Service from issuing the Bell commemorative stamp on the ground that Meucci was the true inventor of the telephone. LaCourte said he intends to keep alive his drive to have Meucci similarly honored by a post office commemorative stamp, and that he harbors no ill will toward Bell. "I can prove Meucci was the inventor — plain and simple. Bell just became a millionaire with Meucci's invention."

Porno Phone Service Busted

Associated Press

In the first federal prosecution of its kind, a 23-count indictment has been returned charging a New York corporation (Carlin Communications Inc.) and four individuals with running a pornographic telephone service that allegedly was dialed by some Utah children. The official charge was interstate transportation of obscene matter.

"Convictions in this case would challenge the phone-sex industry, which has spread across the country during the past two years," U.S. Attorney Brent Ward said.

The Federal Communications Commission ruled in June of 1984 that commercial operators of "dial-a-porn" phone services must restrict children's access by limiting hours of operation and the method of paying for the service.

IRS Drives Telco To Drink

Philadelphia Inquirer

An enormous volume of calls from taxpayers seeking information from the Internal Revenue Service on their late tax refunds threatened to knock out telephone service to much of Center City Philadelphia in April, according to Bell of Pennsylvania officials.

To prevent the massive number of inquiries to the IRS from overloading the 40,000 telephone access lines serving half of Center City, Bell technicians had for a number of weeks been electronically diverting millions of calls. "The traffic had been coming in at such a rapid rate that it virtually ripped our system apart. If we didn't [divert phone calls], it would have put the office in real jeopardy — the ability of people to make calls or receive them," said James Killeen, an engineer in the company's electronic-switching division.

During one 15-minute period, Bell was able to count at least 6,000 calls made to two IRS numbers. But officials say the actual volume of additional calls being made to the IRS numbers at the same time was so heavy that it was beyond the capabilities of their computerized monitoring equipment.

The crush of telephone calls was spurred by the IRS's delay in processing millions of tax returns filed at the agency's Roosevelt Boulevard service center. As of late April, an estimated one million returns had not been opened, according to the agency. A spokesman for the IRS said they were unaware of the problem with telephone-call volume.

The IRS maintains 34 access lines for its toll-free tax information number. The agency has 23 access lines for its "Tele-tax" line (2155928946), which taxpayers are supposed to be able to call and punch in their Social Security number on the telephone to obtain information about the status of their tax refunds.

The majority of telephone calls were diverted by Bell with a recording saying "all circuits are busy." And those that got through say they were frequently disconnected.

Occasionally, even stranger things happened on the IRS lines. Once they succeeded in reaching either number, taxpayers said they found themselves talking not to an IRS computer or a telephone assister, but to other taxpayers.

Jersey Wins Wiretap Race Again

Newark Star-Ledger

New Jersey telephones were far more likely to be tapped by law enforcement authorities than those in any other state last year, a distinction that has been noted in the last seven annual wiretap reports issued by the Administrative Office of the U.S. Courts.

Michael Bozza, assistant director of criminal justice in the state Attorney General's Office, reiterated that New Jersey's zealous use of electronic surveillance demonstrates that law enforcement authorities are especially aggressive in investigating organized crime.

According to the report, New Jersey authorities sought and received court approval for 151 taps in 1984 — an increase of 2% over the 1983 total. The jump reverses a trend that had brought the number of wiretaps down steadily in recent years.

New Jersey was followed in the ranking by New York, which used 122 wiretaps, Florida, with 58, and Pennsylvania, with 46. No other state had more than 23 wiretaps authorized last year. More than 40 percent of the nation's wiretaps were authorized in New Jersey, New York, and Florida, the report said.

AT&T Computer Caught Stealing

The New York Times

The BellSouth Corporation has been told by AT&T that as many as 41,000 business customers might have been improperly assigned to AT&T long distance service.

BellSouth has filed plans with the Department of Justice to correct the results of an AT&T computer program that erroneously assigned service under the equal-access program mandated by the breakup of the Bell System.

Meanwhile, Nynex says that a previously reported figure of some 19,000 business customers in the Nynex region improperly assigned to AT&T long distance service had grown to about 47,000 as a result of additional programming mistakes reported by AT&T.

In a related development, the Bell Atlantic Corporation said it would alter its method of allocating callers to long-distance carriers. Beginning in September, Bell Atlantic said customers who did not choose a long-distance carrier after having two opportunities to do so would be assigned a carrier by Bell Atlantic. Previously, customers who did not make a choice were left with AT&T.

LETTERS AND QUESTIONS

I live in the 215 (Philadelphia area) area code and made a directory assistance call to 609 (South Jersey) to get an Atlantic City number, and then placed the call to the actual number. The actual call naturally appeared on my AT&T portion of the bill. But the killer is that the directory assistance call, supposedly one of an allotment of 2 free DA calls via AT&T, came up as a $.50 charge on the Bell of Pa. portion of the bill! Apparently, Bell of Pa. owns a special exception to the inter-state rules and handles calls to 3 neighboring NJ counties. Since directory assistance is probably handled out of Trenton, my DA call got handled and billed by Bell of Pa. You won't believe how AT&T handles this situation--you have to call them up (1-800-222-0300) and they look you up to make sure you made the equivalent *required* call, then credit your AT&T account! Since this is a totally manual operation, and since we the public have never been told of this strange hack, chances are good that Bell of Pa. is collecting gobs of half dollars which their customers really do not owe; furthermore, when a watchful customer does go through the requisite manual process, it seems as if Bell of Pa. ends up with AT&T's money. AT&T also seems to be able to see the Bell of Pa. portion of the bill on *their* computer terminals. Why do I get the impression that AT&T is *not* as severed from the operating companies as they would have us believe? Hmmmm...

I recently had my telephone disconnected due to the fact that my roommate had forgotten to pay the bill. I have no dispute with the billing, however, my question is: My PacTel bill was around $15. We had paid off $85 of our bill, leaving a balance of $82. Therefore, I would assume, we had paid our debt to PacTel and only owed money to AT&T. Now at the bottom of my monthly long distance statement, it says that the billing is only provided as a service to AT&T, with whom Pacific Telephone has no connection. If this is the case, under what authority did they cut off my telephone service. If I fail to pay my MCI bill, would PacTel cut me off? Shouldn't I just be cut off from AT&T's lines, and collecting is their problem? Just a little more confusion resulting from the break-up.

Nobody should really be surprised when two companies that were once one do each other favors. We've heard quite a few similar tales and would like to hear more. Perhaps we could gather them together and go to the right person and get these companies in a big pile of trouble. Nothing like phreak revenge, they say.

I am writing in reply to James (Feb. 85 issue) and other readers who have conspired to call merchant ships on the high seas. You may dial them direct, and pay $10 per minute, by dialing 011 + ocean code + ship's terminal number. The ocean codes are: 871 Atlantic, 872 Pacific, and 873 Indian ocean. The ship's terminal number can be discovered by asking your telco operator for the Marisat operator (in Alaska, dial 211 and ask for the marine operator), who has a directory of all the ships (except the CIA ships, which someone forgot to include...). Ship's numbers are seven digits, all beginning with '1' (e.g. 1501604, AT&T's Cable Ship Long Lines). The blue box crowd can reach the international operators by beeping KP + 160 + ocean code + ST. These clones sit at TSPS consoles, but have neither ship's directories nor understanding of the Marisat network.

The folks at Comsat's Maritime Services department are more than happy to supply the shipping and offshore industry with ship's directories and Marisat users guides free of charge. Call (800) 424-9152, anytime of day.

And while you're ka-chirping across the network, you'll be amused to find out that the Rate & Route operators have moved, and are now only available on (800) 141-1212. If you're driving cross-country this summer, then be sure to stop in one of those two-pay-phone towns and try dialing this routing. It's amazing how many independent telcos pass you right through!

Rusty Diode

In your February 1985 issue, you told James that to call ships at sea, he must first call the operator and then ask to be connected to the high seas operator. This is nice, but it's awful damn slow, and most Bell clones won't know how to connect you anyways.

To call ships at sea, you must first call one of these toll-free numbers. Either the Marisat operator at 800-243-3640 (or 264-9090 in CT) or Maritime services at 800-424-9152. Be prepared to give the op your billing information, plus the name of the ship and seven digit ID number.

Most phreaks will route this call through a PBX or blow off another WATS number and then box the call. There have been times when some enterprising phreaks decided to bill their calls to the local CO. Of course, we all know that *2600* readers would not do this.

I am writing this letter because I found some humor in an old tv commercial that I saw several months ago. The commercial was one by AT&T. It was titled "AT&T is in Cereal". The commercial was about the toll-free number that can be reached to find the treasure from a map included in a box of cereal. Big deal you say! The catch is, the name brand of the cereal was Captain Crunch. I find that interesting because, if you remember, Captain Crunch is the cereal that contained the little blue whistle that is now known as a blue box. And everyone knows how much trouble that little device caused AT&T. It just goes to show that even the big guys can do something against their will for the right price!

The Silver Sabre

Just one correction on that. The whistle was not a blue box (can you imagine finding a complete blue box in a box of cereal?!). The whistle was able to produce a pure 2600 hertz tone, which seized long distance trunk lines, thus enabling blue box tones to be utilized. The 2600 hertz button is the most important part of a blue box, unless you live in an area that allows you to dial right into an open trunk, thus making it unnecessary to seize one.

Got something on your mind? Then write to: 2600 Letters Editor, Box 99, Middle Island, NY 11953-0099. You can also leave us electronic mail on our official bulletin board, The Private Sector (2013664431). If you have a problem with your subscription or a question, write to: 2600, Box 752, Middle Island, NY 11953-0752 or call us at 5167512600.

The 2600 Information Bureau

THIS IS A LIST OF 800 PREFIXES
IN ORDER BY STATE.

ALABAMA	633	(205)
ALASKA	544	(907)
ARIZONA	528	(602)
ARKANSAS	643	(501)
CALIFORNIA	227	(415)
	421	(213)
	423	(213)
	854	(714)
	824	(916)
	538	(408)
	235	(805)
	344	(209)
	358	(707)
COLORADO	525	(303)
	255	(303)
CONNECTICUT	243	(203)
DELAWARE	441	(302)
DISTRICT OF COLUMBIA	424	(202)
	368	(202)
FLORIDA	327	(305)
	237	(813)
	874	(904)
GEORGIA	841	(912)
	241	(404)
	554	(404)
HAWAII	367	(808)
IDAHO	635	(208)
ILLINOIS	621	(312)
	323	(312)
	637	(217)
	435	(815)
	447	(309)
	851	(618)
INDIANA	457	(812)
	348	(219)
IOWA	553	(319)
	247	(515)
	831	(712)
KANSAS	835	(316)
	255	(913)
KENTUCKY	626	(502)
	354	(606)
LOUISIANA	535	(504)
	551	(318)
MAINE	341	(207)
MARYLAND	368	(301)
MASSACHUSETTS	343	(617)
	225	(617)
	628	(413)
MICHIGAN	253	(616)
	521	(313)
	338	(906)
	517	(248)
MINNESOTA	328	(612)
	533	(507)
	346	(218)
MISSISSIPPI	647	(601)
MISSOURI	821	(816)
	325	(417)
	641	(314)
MONTANA	548	(406)
NEBRASKA	228	(402)
	445	(308)
NEVADA	634	(702)
	648	(702)
NEW HAMPSHIRE	258	(603)
NEW JERSEY	257	(609)
NEW MEXICO	545	(505)
NEW YORK	223	(212)
	847	(607)
	221	(212)
	431	(914)
	828	(716)
	645	(516)
	448	(315)
	833	(518)
NORTH CAROLINA	334	(919)
	438	(704)
NORTH DAKOTA	437	(701)
OHIO	321	(216)
	543	(513)
	537	(419)
	848	(614)
OKLAHOMA	654	(405)
	331	(918)
OREGON	547	(503)
PENNSYLVANIA	523	(215)
	345	(215)
	458	(814)
	245	(412)
	233	(717)
PUERTO RICO	468	(809)
RHODE ISLAND	556	(401)
SOUTH CAROLINA	845	(803)
SOUTH DAKOTA	843	(605)
TENNESSEE	251	(615)
	238	(901)
TEXAS	527	(214)
	433	(817)
	531	(512)
	231	(713)
	351	(713)
	858	(806)
UTAH	453	(801)
VERMONT	451	(802)
VIRGINIA	446	(804)
	368	
	336	(703)
VIRGIN ISLANDS	524	(809)
WASHINGTON	426	(206)
	541	(509)
WEST VIRGINIA	624	(304)
WISCONSIN	356	(608)
	558	(414)
WYOMING	443	(307)

The list above was posted on The Private Sector by AX MURDERER. It should be noted that with modern methods of phone routing and billing this list cannot be depended on as complete and accurate. These exchanges are now only generally found in the areas or area codes listed, because with the newer technology there are relatively few restrictions as to the actual phone number assignments for toll free service. In some of these exchanges it is possible to dial the exchange and then "0000", and the location will be read off by some recorded clown somewhere.

Out of the Inner Circle—A REVIEW

(continued from page 2-34)

is an important element of the book where Landreth describes the psychology and thought processes of technology's foe, the hacker. He tries to classify them, so he can refer to them later: the novice; the student, which Landreth considers himself to be; the tourist; the crasher; and the thief. He describes various methods of hacking in "How a Hacker Hacks" such as guessing defaults, using help files and demos. He then goes on to discuss different general types of computers and peripherals as well as operating systems, what account privileges are, what security is, the role of the sysop, and various hacker scenarios. The book is full of dramatic digressions into the activity of a hard core hacker, who may spend as much as a year to break into a system, may return to enter a system with 100 or more "friends", or may even pretend to poll employees outside the target company as they go to work in order to find out user names and any personal information that might be used as passwords.

Out of the Inner Circle is written for these management types, who will read and read, get nervous, and then lean on the system operators to beef up security. Landreth also refers to sysops who do not mind chatting with hackers, as well as system designers who may build trap doors into the system that they set up for you. Then one day they may call up your computer, enter your system through the trap door that they installed and do whatever they wish. Now, these management types may start keeping an eye on their computer experts as well as company security. Out of the Inner Circle is also full of vignettes which may sound commonplace to the average hacker, but that should scare the businesspeople of America - descriptions of the activities of crashers who try to erase files or halt systems and of hackers reading personal documents and entering corporate computers.

Landreth often makes mention of a system by its value. "Someone is trying to break into your million dollar computer..." he might say. This is the language that corporate America speaks. Landreth is not very worried that someone may be looking at your credit information, and even less worried that there exist companies that own and sell it.

But, basically, Landreth fulfills the purpose of the book in two chapters: "Make the Most of What You've Got", and "Telltale signs". Together they would make a good guide of simple suggestions that could prove invaluable to sysops, system designers, and computer security consultants. In the latter chapter, Landreth discusses how one could reduce accessibility to spare or unattended terminals, how to reduce the liability of dial-ups, change logon procedures, assign complex passwords, and several other inexpensive procedures that can beef up security and keep out most hackers. In the former, he lists some telltale signs for one to suspect that an intruder has been on the system, such as excessive use of help files, movement of other files, activity in normally dormant accounts, etc. It is these two chapters alone that make the book useful. They contain all that information that hackers know and about which they sometimes remark: "If I was running that system, this is what I would do..." These chapters tell of the basic steps to follow to greatly reduce computer intrusion by hackers. If these suggestions are followed, the total amount of illegal entry may decrease by a substantial percentage. Leaving only the very clever and persistent hackers to examine corporate America from the inside. This in turn would finally give some credibility to the myth of the computer wiz-kid.

Then again, this book can be taken in another ways: Only a few weeks ago, according to *2600* reporter Hunter Alexander, P. Michael Nugent of the Electronic Data Systems Corporation fumed about Out of the Inner Circle before the crime subcommittee of the House calling it a "how to do it [computer crime]. How do I handle that?" he asked Rep. William Hughes (D. N.J.). Mr. Nugent ought to read the book before the hackers do, if he is so worried.

israeli phone system

(continued from page 2-33)

fun as here - when one party picks up the phone, the other is locked out, and cannot interfere or use the line.

Getting your phone service fixed can also be a trying task. Flakiness is about the best word that describes their telco's repair branch. After one or two complaints, if you're lucky, the problem might get fixed, and not recur the next day. It is just about useless to complain about repair problems to a supervisor, since the supervisor's phones are always busy or never answered. Social engineering (such as pretending to be a reporter or other person with clout) is about the only reliable way of getting your complaints resolved.

The phone system is also the source of one of the many national paranoias. "I can't talk about that over the phone" is heard incredibly often. Perhaps it's because Israel is a small country with many noticeable security precautions (for example, you must open your bag in front of a security guard whenever walking into any large establishment so they can check you for ammunition or explosives). Some people almost routinely assume that their conversations are monitored, just like a lot of phone phreaks over here always think.

ARPANET DIALUPS

4153275220
3019483850

SOME CORPORATE MODEMS

8005263714
8003430999
8003431360
8008211200
8003254154
8003438849
8003211570
8003211646
8003256397

SYSTEMATICALLY SPEAKING

Say Goodbye to Meter Readers

Associated Press

The New York Telephone Company has asked the State Public Service Commission to approve a plan to read utility meters by telephone, a service that could make the door-to-door meter reader a figure of the past.

A statement issued by the company said regular telephone service would be unaffected by the meter-reading service. The service would make readings only on telephone lines that were not in use, and would automatically disconnect if a call came in during a reading. Each reading would take about two seconds, a New York Telephone spokesperson said, and would probably take place at night.

Bob Loftus, a spokesman for Brooklyn Union Gas Company, said, "We'd be able to reduce operating costs, we think. And, of course, our customers would have convenience, since they would not need to be at home. And it would eliminate estimated billing."

Officials for the union representing Brooklyn Union Gas meter readers could not be reached for comment.

Thai Phone Books a Hot Issue

Wall Street Journal

An AT&T unit filed a $95.6 million lawsuit against a GTE unit, escalating a battle over the right to publish Thailand's telephone directories.

The suit, filed by AT&T International Inc. in Bangkok, Thailand, alleges that actions by GTE Directories Corp. and other defendants have caused "severe damage to the reputation" of AT&T International in Thailand and other countries.

In February, AT&T International won fierce bidding for the right to publish Thailand's directories for the next five years. The loser was GTE Directories Corp., whose Thai unit had published Thailand's phone books for the past 17 years.

In March, GTE Directories filed a $31.4 million suit against AT&T International, alleging it had committed "wrongful acts" in connection with the bidding.

New Tracking Device For Cars

The New York Times

Seven years ago, William R. Reagan wrote out an invention disclosure, the first step toward a patent. With all the police cruisers and communications networks and computers in this country, he thought, there should be some way to equip an automobile with a transmitting device that the police could home in on should the car be stolen.

Today, Mr. Reagan is responsible for just such a device. A police cruiser equipped with a tracking unit can pick up the signal two or three miles away, lock in on it, and track it through woods, fields, subdivisions, or city streets, right to the car. In 550 tests in the last four months, the Massachusetts State Police have found the hidden car every time.

By an agreement reached with the state, Mr. Reagan has installed about $300,000 worth of equipment that will remain in state police cruisers and facilities.

When a car is reported stolen, the police entry in the crime computer automatically causes a special signal to be broadcast from police radio towers across the state. When the signal reaches the transmitting device in the stolen car, the device begins to emit its own silent pulse, which can be picked up by police cruisers with tracking units. The signal flashes the car's code name on the cruiser's console. The officer in the cruiser gives that name to the police dispatcher, who uses it to get the stolen car's description from the crime computer. He gives that description to the officer in the cruiser, and so, as the cruiser homes in on the signal, the officer knows what car to look for.

Massachusetts governor Michael D. Dukakis commented, "[My ultimate goal is] eleven million cars a year coming out of Detroit equipped with this."

Problems for New Pay Phones

Forbes

Since the FCC approved the sale of pay phones in the summer of 1984, new competitors have sold or installed more than 10,000 privately owned coin-operated phones. Many in the industry expect upwards of one million to be in use by 1990, replacing at least some of the 1.8 million phone company quarter-eaters currently in operation.

A technological hurdle is still to be cleared, though. Until recently none of the so-called smart pay phones have been able to determine when a call is unswered, and thus when to gobble the coins. To collect the money, the phones typically require users to push a button once the connection is made before they can be heard by the other party. Many people get confused and lose their money. "Violently smashed phones are a major problem," says William Moorehead, a specialist on the industry for the Partridge Group consulting firm in Washington, D.C.

TINA Message Service

Radio Electronics

A new communications service, which is expected to make it possible for small businesses to send and receive international messages for a small fraction of the cost of Telex or similar services, has been initiated by Service Systems Technology (SST) of Marina del Rey, CA and Milan, Italy.

Known as TINA International Message Service, the new system has one limitation as compared with Telex or similar services: Communication is between subscribers in U.S. or foreign "gateway cities," or more specifically, from the computer of a subscriber to the computer at his other "electronic mailbox."

A subscriber dials a local number to get on an international network, then sends his message through a modem attached to his telephone. The network is that of INFONET, which has offices worldwide.

Cost of the service, which includes two "electronic mailboxes" and two hours of computer time is $99.60 per month. That charge, says SST, gives subscribers the amount of service that would cost about $2200 by conventional services. Extra computer connect time is obtainable at $58.60 per hour. Extra electronic mailboxes and user ID's are $10 per month.

AT&T Contractual Obligations

Combined News Sources

AT&T is making its employees sign a new contract which prohibits the disclosure of proprietary information outside the company. In addition, the contract covers inventions made as a result of employment, as well as inventions in "all areas in which AT&T does business or in which the company might be reasonably involved in the future." It is forcing this "agreement" not only to new employees but to its present employees.

"Call Me" Card

Combined News Sources

AT&T will soon introduce a credit card that can only be used for calling home. The card should eliminate any chance of telephone fraud on credit card numbers. In addition, it is expected to reduce phone bills by removing incentive to call anyplace else.

FROM SHERWOOD FOREST: INTRO TO HACKING

This article, "The Introduction to the World of Hacking" is meant to help you by telling you how not to get caught, what not to do on a computer system, what type of equipment should I know about now, and just a little on the history, past present future, of the hacker.

***

Welcome to the World of Hacking! We, the people who live outside of the normal rules, and have been scorned and even arrested by those from the "civilized world", are becoming scarcer every day. This is due to the greater fear of what a good hacker (skill wise, no moral judgements here) can do nowadays, thus causing anti-hacker sentiment in the masses. Also, few hackers seem to actually know about the computer systems they hack, or what equipment they will run into on the front end, or what they could do wrong on a system to alert the "higher" authorities who monitor the system.

This article is intended to tell you about some things not to do, even before you get on the system. We will tell you about the new wave of front end security devices that are beginning to be used on computers. We will attempt to instill in you a second identity, to be brought up at time of great need, to pull you out of trouble. And, by the way, we take no, repeat, no, responsibility for what we say in this and the forthcoming articles. Enough of the bullshit, on to the fun:

***

After logging on your favorite bbs, you see on the high access board a phone number! It says it's a great system to "fuck around with!" This may be true, but how many other people are going to call the same number? So; try to avoid calling a number given to the public. This is because there are at least every other user calling, and how many other boards will that number spread to?

If you call a number far, far away, and you plan on going thru an extender or a re-seller, don't keep calling the same access number (i.e. as you would if you had a hacker running), this looks very suspicious and can make life miserable when the phone bill comes in the mail. Most cities have a variety of access numbers and services, so use as many as you can. Never trust a change in the system... The 414's, the assholes, were caught for this reason: when one of them connected to the system, there was nothing good there. The next time, there was a trek game stuck right in their way! They proceeded to play said game for two, say two and a half hours, while TELENET was tracing them! Nice job, don't you think? If anything looks suspicious, drop the line immediately!! As in, YESTERDAY!! The point we're trying to get across is: if you use a little common sense, you won't get busted. Let the little kids who aren't smart enough to recognize a trap get busted, it will take the heat off of the real hackers. Now, let's say you get on a computer system...it looks great, checks out, everything seems fine. Ok, now is when it gets more dangerous. You have to know the computer system (see future issues of this article for info on specific systems) to know what not to do. Basically, keep away from any command which looks like it might delete something, copy a new file into the account, or whatever? Always leave the account in the same status you logged in with. Change *NOTHING*...if it isn't an account with priv's, then don't try any commands that require them! All, yes ALL, systems are going to be keeping log files of what users are doing, and that will show up. It is just like dropping a trouble-card in an ESS system, after sending that nice operator a pretty tone. Spend no excessive amounts of time on the account in one stretch. Keep your calling to the very late night if possible, or during business hours (believe it or NOT!). It so happens that there are more users on during business hours, and it is very difficult to read a log file with 60 users doing many commands every minute. Try to avoid systems where everyone knows each other, don't try to bluff. And above all: NEVER act like you own the system, or are the best there is. They always grab the people whose heads swell...

There is some very interesting front end equipment around nowadays, but first let's define terms...

By front end, we mean any device that you must pass thru to get at the real computer. There are devices that are made to defeat hacker programs, and just plain old multiplexers. To defeat hacker programs, there are now devices that pick up the phone and just sit there... This means that your device gets no carrier, thus you think there isn't a computer on the other end. The only way around it is to detect when it was picked up. If it picks up after the same number ring, then you know it is a hacker-defeater. These devices take a multi-digit code to let you into the system. Some are, in fact, quite sophisticated to the point where it will also limit the user name's down, so only one name or set of names can be valid logins after they input the code... Other devices input a number code, and then they dial back a pre-programmed number for that code. These systems are best to leave alone, because they know someone is playing with their phone. You may think "But I'll just reprogram the dial-back." Think again, how stupid that is... Then they have your number, or a test loop if you were just a little smarter. If it's your number, they have your balls (if male...), if its a loop, then you are screwed again, since those loops are *monitored*.

As for multiplexers... What a plexer is supposed to do is this: the system can accept multiple users. We have to time share, so we'll let the front-end processor do it... Well, this is what a multiplexer does. Usually they will ask for something like "enter class" or "line:". Usually it is programmed for a double digit number, or a four to five letter word. There are usually a few sets of numbers it accepts, but those numbers also set your 300/1200 baud data type. These multiplexers are inconvenient at best, so not to worry.

A little about the history of hacking: hacking, by our definition, means a great knowledge of some special area. Doctors and lawyers are hackers of a sort, by this definition. But most often, it is being used in the computer context, and thus we have a definition of "anyone who has a great amount of computer or telecommunications knowledge." You are not a hacker because you have a list of codes... Hacking, by our definition, has then been around only about 15 years. It started, where else but, MIT and colleges where they had computer science or electrical engineering departments. Hackers have created some of the best computer languages, the most awesome operating systems, and even gone on to make millions. Hacking used to have a good name, when we could honestly say "we know what we are doing". Now it means (in the public eye): the 414's, Ron Austin, the NASA hackers, the Arpanet hackers... All the people who have been caught, have done damage, and are now going to have to face fines and sentences. Thus we come past the moralistic crap, and to our purpose: educate the hacker community, return to the days when people actually knew something...

***

A program guide: Three more articles will be written in this series, at the present time. Basics of Hacking I: DEC's Basics of Hacking II: VAX's (UNIX) Basics of Hacking III: Data General. It is impossible to write an article on IBM, since there are so many systems and we only have info on a few... This article has been written by: The Knights of Shadow